



Documento di ePolicy

BSIC85400N

I.C. MARCHENO

VIA E. RINALDINI 5 - 25060 - MARCHENO - BRESCIA (BS)

Mariateresa Boniotti

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del [Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente](#) e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

1. **Presentazione dell'ePolicy**

1. Scopo dell'ePolicy
2. Ruoli e responsabilità
3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. **Formazione e curriculum**

1. Curriculum sulle competenze digitali per gli studenti
2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
4. Sensibilizzazione delle famiglie e Patto di corresponsabilità

3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**

1. Protezione dei dati personali
2. Accesso ad Internet
3. Strumenti di comunicazione online
4. Strumentazione personale

4. **Rischi on line: conoscere, prevenire e rilevare**

1. Sensibilizzazione e prevenzione
2. Cyberbullismo: che cos'è e come prevenirlo
3. Hate speech: che cos'è e come prevenirlo
4. Dipendenza da Internet e gioco online
5. Sexting
6. Adescamento online
7. Pedopornografia

5. **Segnalazione e gestione dei casi**

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi

all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

Nello specifico, l'istituto ha aderito al progetto ePolicy di Generazioni Connesse, consapevole dell'importanza di "darsi" uno strumento pensato ad hoc per la gestione e l'utilizzo delle tecnologie digitali sia per adeguarsi alla didattica integrata sia per sistematizzare protocolli e regolamenti già presenti. Il periodo vissuto nei mesi della Didattica a distanza, ha imposto alla scuola un radicale cambiamento e un necessario ripensamento della didattica che deve tener necessariamente conto dell'utilizzo delle tecnologie digitali e, di conseguenza, dell'importanza di dotarsi di norme e procedure per garantire un uso positivo, corretto e sicuro in ambiente scolastico delle tecnologie dell'informazione e della comunicazione ICT. Nello stesso tempo, è indispensabile attivare tutte le misure di prevenzione, rilevazione e gestione delle problematiche connesse ad uso non consapevole delle tecnologie digitali.

1.2 - Ruoli e responsabilità

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

- **Il Dirigente Scolastico**

Il Dirigente Scolastico si adopera per garantire la sicurezza, anche online, di tutti i membri della comunità scolastica. Si forma adeguatamente sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; promuove la cultura della sicurezza online attraverso corsi di formazione specifici per le figure scolastiche sull' utilizzo positivo e responsabile delle ICT. Il Dirigente Scolastico ha inoltre la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali. Partecipa alla stesura di tutti i regolamenti d'istituto, orientandone l'indirizzo e armonizzandoli con la regolamentazione già in uso. E' titolare unico del trattamento dei dati degli alunni e del personale scolastico.

- **L'Animatore digitale**

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento alla protezione e gestione dei dati

personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale"; inoltre, può monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle ICT a scuola e avere il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

- Il Referente bullismo e cyberbullismo

Tale figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio, dove presenti. Favorisce iniziative condivise con il territorio in occasione delle giornate dedicate; interviene e coordina interventi di sensibilizzazione nelle classi filtro.

- I Docenti

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle ICT e della Rete. Si impegnano, innanzitutto, ad integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

- Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola.

- Gli Studenti e le Studentesse

gli Studenti e le Studentesse, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola si impegnano ad imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le; partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle ICT e della Rete.

- I Genitori

I Genitori, in continuità con l'Istituto scolastico, si impegnano ad essere partecipi e

attivi nelle attività di promozione ed educazione sull'uso consapevole delle ICT e della Rete, nonché sull'uso responsabile dei device personali; si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le ICT e la Rete e comunicano con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. È estremamente importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto.

- Gli Enti educativi esterni e le associazioni

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola dovranno conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle ICT; dovranno, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Per quanto concerne le regole di comportamento per i soggetti esterni che erogano attività educative nell'istituto si fa riferimento alla documentazione prodotta dal DPO d'istituto.

1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Le azioni pensate per la condivisione e comunicazione dell'ePolicy alla comunità scolastica, oltre a quelle già specificate, sono le seguenti:

- invito del Dirigente Scolastico alla lettura attenta del documento disponibile nel sito istituzionale e condivisione di eventuali correzioni da raccogliere per le successive modifiche e aggiornamenti periodici
- presentazione agli studenti e alle studentesse durante i lavori di approfondimento della Giornata contro il Bullismo alla quale aderisce tutto l'istituto
- presentazione ai genitori da parte del gruppo ePolicy
- invio del documento agli enti territoriali che collaborano con la scuola

1.5 - Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni in relazione ai regolamenti e normative vigenti.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

I regolamenti d'istituto vengono allegati alla ePolicy.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

In condizioni standard si prevede un monitoraggio annuale in occasione della verifica e

approvazione del PTOF.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il documento ai docenti e ai genitori

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Capitolo 2 - Formazione e curriculum

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più “intuitivo” ed “agile” rispetto agli adulti, ma non per questo sono dotati di maggiori “competenze digitali”.

Infatti, “la competenza digitale presuppone l’interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l’alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l’alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l’essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico” ([“Raccomandazione del Consiglio europeo relativa alla competenze chiave per l’apprendimento permanente”](#), C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale.

Da qui la necessità di dotare il nostro Istituto di un Curriculum Digitale ossia di un percorso didattico progettato per sviluppare competenze digitali, di facile replicabilità, utilizzo e applicazione e necessariamente verticale e trasversale. Il curriculum digitale conterrà anche riferimenti all'introduzione dello studio del pensiero computazionale e del coding come approccio trasversale, in coerenza con le indicazioni nazionali per il curriculum.

2.2 - Formazione dei docenti

sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica deve diventare un processo permanente che deve prevedere anche momenti di autoaggiornamento, di formazione personale o collettiva. L'istituto da alcuni anni organizza corsi con risorse interne con approccio operativo laboratoriale e segnala puntualmente le iniziative legate al Piano Nazionale Scuola Digitale organizzate dall'UST.

Si fa riferimento al Piano di Formazione d'istituto.

2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di

Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Nel corso degli ultimi anni, il nostro Istituto ha organizzato incontri aperti alle famiglie e agli studenti con risorse interne ed enti esterni per sensibilizzare docenti, alunni e genitori sui temi della sicurezza online. Anche nei prossimi anni si continuerà ad utilizzare questo approccio per la sensibilizzazione delle famiglie, con incontri che offriranno occasione di confronto e discussione sui rischi rappresentati dall'uso di cellulari, smartphone e chat line senza un'adeguata formazione in merito ai rischi derivanti da un uso inappropriato di tali dispositivi. Sul sito scolastico saranno resi accessibili i materiali, tra cui guide in formato pdf e video dedicati alle famiglie e ai ragazzi nella bacheca virtuale del sito di "Generazioni connesse". La scuola darà inoltre ampia diffusione, tramite pubblicazione sul sito, del presente documento di e-policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

Il nostro piano d'azioni

AZIONI DA SVILUPPARE NELL'ARCO DELL'ANNUALITÀ 2020/21

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

3.1 - Protezione dei dati personali

“Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino”.

(cfr. <http://www.garanteprivacy.it/scuola>).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il “corretto trattamento dei dati personali” a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

La diffusione sempre maggiore di smartphone tra i giovanissimi, l'uso di tablet a scopo didattico, la condivisione online di contenuti didattici, l'uso del registro elettronico, l'eventualità di gruppi whatsapp tra studenti/esse, genitori, docenti o tra insegnanti e studenti/esse, obbliga la scuola ad avere un'attenzione particolare non solo alla privacy in generale, ma anche alla gestione della privacy legata all'uso dei nuovi dispositivi. La velocità, l'immediatezza con cui si risponde ai messaggi o si condividono foto o video, può far perdere il controllo di dati personali e mettere a rischio la reputazione e la sicurezza dei soggetti coinvolti quindi la nostra scuola ha raccolto la sfida per costruire le condizioni per un futuro migliore delle nuove generazioni impegnandosi anche nel "corretto trattamento dei dati personali".

I dati personali che il nostro istituto si impegna a tutelare sono i seguenti:

- dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitiva, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) comprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Le numerose informazioni sensibili sugli studenti e le studentesse, o sulle loro famiglie, che vengono trattate giornalmente nel nostro Istituto sono tutelate da un apposito REGOLAMENTO al fine di preservare la riservatezza e la dignità della persona, in particolare quando sono coinvolti soggetti minorenni.

Tale documento adottato nel 2018 dagli organi competenti sottolinea come la protezione dei dati personali sia un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal [Regolamento \(UE\) 2016/679 del Parlamento europeo e del Consiglio](#), del 27 aprile 2016 (relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Il regolamento PRIVACY recepisce, adeguandosi, quindi, al cosiddetto GDPR (General Data Protection Regulation) e al D. Lgs. n. 101/2018

COSA HA DISCIPLINATO?

- Ha preparato l'Informativa per il trattamento dei dati personali che riguarda: alunni e loro famiglie ex art. 13 Regolamento UE 2016/679 ("RGPD"), dipendenti, fornitori, Videosorveglianza, Sito Web, Cookie, didattica e formazione a distanza, protocollo Sicurezza e Salute
- Ha esplicitato la Modulistica

[Modulo per diritto di accesso.pdf](#)

[Modulo segnalazione data breach PA.pdf](#)

[Linee Guida Foto-Video Prodotti Da Privati.pdf](#)

[Linee guida assistenti amministrativi](#)

[Linee guida docenti](#)

[Linee guida collaboratori scolastici](#)

[Linee guida personale tecnico e animatore digitale](#)

- Ha fornito risposta a FAQ e ha inserito i seguenti riferimenti legali essenziali per approfondimenti

[2003-06-30 Dlgs196-2003 con modifiche 2011.pdf](#)

[2006-07-12 dm_305-2006 con allegati.pdf](#)

[2009-06-25 ProvvedimentoGarante-AmministratoriSistema.pdf](#)

[2010-10 Provvedimento in materia di videosorveglianza.pdf](#)

[2014-10 LineeGuidaGarante-LaTrasparenzaSuiSitiWebDellaPA.pdf](#)

[2016-04-27 Regolamento UE 679-2016 con riferimenti ai considerando.pdf](#)

[2016-10 Vademecum La scuola a prova di privacy.pdf](#)

[2017-04-05 WP243 - Linee guida su gli RPD.pdf](#)

[2018-08-10 DLgs 101-2018 adeguamento del DLgs196.pdf](#)

[2018-09 Codice in materia di protezione dei dati personali \(Testo coordinato\).pdf](#)

Inoltre, la scuola non ha solo il compito di tutelare la privacy degli/le studenti/esse e delle loro famiglie, ma anche quello di informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri, a tal proposito organizza e ha organizzato **momenti formativi** rivolti sia al personale che alle famiglie e agli studenti/esse sia in presenza che attraverso **Webinar**.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del

Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le “misure riguardanti l’accesso a un’Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all’interno dell’Unione”.

Il diritto di accesso a Internet è dunque presente nell’ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di “fornire a tutte le scuole le condizioni per l’accesso alla società dell’informazione e fare in modo che il “diritto a Internet” diventi una realtà, a partire dalla scuola”.

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall’altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

INFRASTRUTTURA TECNOLOGICA DELL’ISTITUTO:

L’IC di Marcheno è composto da 14 plessi nei quali l’infrastruttura tecnologica è stata oggetto di continuo miglioramento ed è stata fortemente implementata all’inizio del corrente anno scolastico; ciascuna classe è stata dotata di un computer portatile connesso ad internet, di una Lim con videoproiettore interattivo e di una tavoletta grafica ad uso del docente. A queste attrezzature si aggiungono anche quattro laboratori di informatica e un laboratorio multimediale.

Quasi tutti i plessi sono dotati di una rete internet sufficientemente potente per permettere la connessione contemporanea di tutti gli insegnanti, permangono ancora delle criticità riguardo alla possibilità della connessione di tutti gli studenti. La scuola, in collaborazione con le amministrazioni comunali, sta lavorando per poter implementare la rete e permettere una connessione stabile in grado di fornire, attraverso cablaggio LAN o wireless, un accesso diffuso, in ogni aula, laboratorio, corridoio e spazio comune munito di sistema di sicurezza di rete.

Tale adeguamento è necessario anche in ottica di un potenziamento degli strumenti didattici e laboratoriali necessari a migliorare la formazione e i processi di innovazione delle istituzioni scolastiche; per conoscere nel dettaglio le migliorie auspiccate dall’istituto si rimanda al PTOF 19/20-21/22 (pp.71-72-73-74), reperibile al seguente link.

<https://rb.gy/pvvxda>

AMBIENTE SICURO ANCHE ONLINE

La scuola deve valutare tutti gli aspetti legati alla sicurezza nel momento in cui permette a studenti/esse e docenti l’accesso alla rete tramite i dispositivi della scuola,

tramite la rete scolastica o tramite i dispositivi personali nel caso del BYOD (Bring your own device).

Non è sufficiente prestare attenzione all'infrastruttura hardware e alla rete (wireless e non), ma è necessario considerare anche la sicurezza di tutti gli aspetti che riguardano la gestione degli account degli utenti (in modo differenziato tra studenti, insegnanti e personale amministrativo), il filtraggio dei contenuti (possibilmente in modo differenziato in base all'età) e gli aspetti legali in relazione prevalentemente alla privacy. Questo è l'obiettivo che sottende ad ogni progettazione di rete.

(AZIONE-OBIETTIVO: E' prevista la dotazione di tutto l'istituto di firewall che toglie gaming, social, contenuti dannosi agli studenti, ma non è ancora presente in tutti i plessi..)

Per quanto riguarda la protezione dei dati personali si fa riferimento alla documentazione prodotta dal DPO d'istituto, reperibile al seguente link.

<https://rb.gy/tbd6xw>

Sempre per garantire un accesso sicuro anche online l'istituto lavora appoggiandosi a due importanti piattaforme create appositamente per l'ambiente scolastico: GSuite for Education e Web Spaggiari. Attraverso queste piattaforme è possibile gestire tutto ciò che riguarda le attività didattiche realizzabili in presenza e a distanza.

Entrambi sono sistemi ad accesso limitato e protetto che non consentono la libera registrazione; per accedere alle piattaforme è necessario essere registrato da parte dei suoi amministratori. Questa modalità di partecipazione assicura un buon livello di controllo degli accessi e delle operazioni svolte dagli utenti sul cloud nonché un ottimo controllo della privacy, inoltre non includono annunci promozionali e non utilizzano mai i contenuti o i dati a fini pubblicitari.

Per il dettaglio delle condizioni e norme di utilizzo si richiama il regolamento Gsuite d'Istituto, consultabile al seguente link.

<https://rb.gy/setug4>

L'ANNOSA QUESTIONE DELLA TECNOLOGIA CHE NON FUNZIONA:

L'IC Marcheno si sta muovendo per far sì che la formazione dei docenti non si limiti solo all'uso delle tecnologie digitali nella didattica, ma sia anche sul funzionamento e sull'uso stesso della tecnologia in sé. A tal fine si coinvolgono il tecnico specializzato, l'animatore e il team digitale e qualche docente che per studio o passione ha conoscenze più tecniche da poter condividere coi colleghi.

Le operazioni di gestione, configurazione, backup e ripristino sono affidate alla funzione strumentale e a risorse tecniche interne presenti nell'Istituto, affiancato a ditte tecniche esterne.

Tra le attività previste dal PTOF in relazione al PNSD si fa riferimento alla formazione del personale scolastico e degli studenti nell'ambito delle tecnologie.

PTOF 19/20-21/22 (pp.71-72-73-74, pp.112-119)

<https://rb.gy/pvvxda>

IL REGOLAMENTO SULL'USO DELLE TECNOLOGIE A SCUOLA:

E' fondamentale nel percorso di crescita l'accompagnamento da parte di adulti competenti anche rispetto al mondo online, con l'obiettivo di aiutarli a sviluppare le competenze digitali necessarie alla convivenza civile e al futuro lavorativo di ragazzi e ragazze.

Si richiama a tal proposito il PATTO CORRESPONSABILITA', il REGOLAMENTO D'ISTITUTO e il REGOLAMENTO BYOD.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Le tecnologie digitali possono rappresentare un'opportunità significativa anche in termini di un maggiore coinvolgimento degli studenti o dei genitori, o alla possibilità di usare diversi linguaggi (scrittura, immagini, video etc.). Grazie agli strumenti di comunicazione online possiamo usufruire dell'interattività del mezzo, superare le barriere spazio-temporali, usare un linguaggio multimediale, ipertestuale e accattivante, promuovere la partecipazione e il coinvolgimento dei diversi attori in gioco nel processo educativo (dai ragazzi ai genitori).

La DS coordina la comunicazione interna ed esterna del nostro Istituto al fine di trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che la scuola porta avanti.

Ogni docente è responsabile del proprio username e della propria password di accesso al registro elettronico e delle password d'accesso alla rete wifi dell'Istituto. In caso di

smarrimento o dimenticanza i docenti devono rivolgersi alla segreteria e far presente il problema. A tutto il personale, docente e non docente, è stato raccomandato di non salvare le password nei browser se gli strumenti vengono utilizzati da più persone e di effettuare sempre il logout dai siti a cui si accede con login e dalle caselle di posta personali. In ogni caso è consigliata la navigazione in modalità incognito del browser sulle periferiche della scuola (PC, notebook, tablet, ecc.). Si invitano altresì i docenti ad una custodia responsabile di tutte le credenziali di accesso con password segrete, alfanumeriche e sicure, cambiate almeno ogni tre mesi.

Gli strumenti di comunicazione online utilizzati dalla nostra scuola sono i seguenti:

- **Per la comunicazione esterna:**

il sito web della scuola (www.icmarcheno.it)

il registro elettronico con tutte le sue funzionalità che permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- udienze (prenotazioni colloqui individuali);
- eventi (agenda eventi);
- comunicazione varie (comunicazioni di classe, comunicazioni personali): vedi ad esempio la bacheca.

Tutte le comunicazioni scuola-famiglia contenenti dati sensibili sono visibili esclusivamente da parte della famiglia dell'alunno interessato e non dal resto della classe

la piattaforma G Suite for Education, con le sue app incluse: e mail (ad ogni alunno è assegnato dal Dirigente scolastico, previa richiesta scritta, un indirizzo email del tipo nome.cognome@www.icmarcheno.edu.it utilizzato per eventuale invio o ricevimento di posta a scopi didattici), drive, meet, classroom...

le e-mail d'istituto: L'account di posta elettronica istituzionale (bsic85400n@istruzione.it) utilizzato ordinariamente dagli uffici amministrativi, sia per

la posta in ingresso che in uscita.

- **Per la comunicazione interna:**

il sito web della scuola;

il registro elettronico con tutte le sue funzionalità;

la piattaforma G Suite for Education;

le e-mail d'istituto;

le mail personali;

Whatsapp per le chat informali fra docenti o gruppi.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne, come avviene generalmente fra i docenti mediante ad esempio l'uso di gruppi whatsapp o telegram, è importante ricordare quello che si può definire "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare

La rete wi-fi è protetto da password in possesso esclusivo dei docenti che utilizzano quotidianamente i computer all'interno delle classi.

Le operazioni di gestione, configurazione, backup e ripristino sono affidate all'animatore digitale e a risorse tecniche interne presenti nell'Istituto.

Tutti i docenti dell'istituto possiedono una e-mail della scuola del tipo: nome.cognome@www.icmarcheno.edu.it. Gli alunni sono dotati di un indirizzo di posta elettronica della scuola del tipo: nome.cognome.s@www.icmarcheno.edu.it. La dotazione di indirizzi di posta elettronica sia dei docenti che degli alunni appartiene all'infrastruttura delle Google Suite for Education.

Ogni docente è responsabile del proprio username e della propria password di accesso al registro elettronico e delle password d'accesso alla rete wifi dell'Istituto. In caso di smarrimento o dimenticanza i docenti devono rivolgersi alla segreteria e far presente il problema. A tutto il personale, docente e non docente, è stato raccomandato di non salvare le password nei browser se gli strumenti vengono utilizzati da più persone e di effettuare sempre il logout dai siti a cui si accede con login e dalle caselle di posta personali. In ogni caso è consigliata la navigazione in modalità incognito del browser sulle periferiche della scuola (PC, notebook, tablet, ecc.). Si invitano altresì i docenti

ad una custodia responsabile di tutte le credenziali di accesso con password segrete, alfanumeriche e sicure, cambiate almeno ogni tre mesi.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente **ePolicy** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Partendo dall'emergenza in atto, che ha richiesto un estremo impegno nell'uso della strumentazione tecnologica personale, l'istituto si è adoperato con grande solerzia ed efficacia per ottenere tutti i dispositivi da rendere disponibili a quegli alunni che per varie ragioni non ne dispongono e la partecipazione dei quali sarebbe gravemente compromessa dalla mancanza del mezzo informatico a disposizione. Attualmente tali dispositivi sono presenti in circa 50 computer portatili, in implementazione numerica, che vengono concessi in comodato d'uso in base ai diritti posseduti e definiti in appositi criteri adottati dagli organi competenti insieme allo stesso regolamento d'accesso alle risorse.

In attesa di accesso con i dispositivi personali a scuola, nel caso del BYOD (Bring your own device), è stata affrontata la necessità di regolarne l'uso attraverso la stesura di un regolamento dedicato attraverso successivi momenti pianificatori che hanno richiesto la soluzione di alcuni punti organizzativi. Si richiama per maggiori dettagli lo stesso documento.

Infine i termini di utilizzo del proprio smartphone a scuola e in classe, richiamando

anche l'azione #15 del PNSD (Scenari innovativi per lo sviluppo di competenze digitali applicate) nell'ottica di potenziare le competenze di cittadinanza digitale, trovano riscontro e regolamentazione nel suddetto **regolamento BYOD**. Unitamente a questo anche tra docenti vi sono scambi di idee e gruppi su applicazioni dello smartphone e si richiamano di seguito le netiquette dedicate.

Uso di strumenti personali dei docenti per chat informali fra docenti o gruppi.

Per le chat informali tra colleghi, si adottano le seguenti **regole condivise**:

- Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);
- Evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- Evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- Non condividere file multimediali troppo pesanti;
- Evitare il più possibile di condividere foto di studenti in chat;
- Indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- Evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esauritivi allo stesso tempo.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).**Scegliere almeno 1 di queste azioni:**

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli
- studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e

le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 - Sensibilizzazione e Prevenzione

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione**.

- Nel caso della **sensibilizzazione** si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
- Nel caso della **prevenzione** si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

Le azioni di sensibilizzazione riguarderanno:

- accrescere la consapevolezza nel gruppo di riferimento circa un determinato tema/bisogno/problema che potrebbe presentarsi in quel gruppo;

- incoraggiare il gruppo a modificare i propri comportamenti rendendoli più funzionali;
- diffondere all'esterno del gruppo di riferimento una certa consapevolezza rispetto all'argomento di interesse;
- facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per lavorare ad un obiettivo comune;
- favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva (promuovere la conoscenza dell'ePolicy nella comunità scolastica).

In sintesi, è opportuno tenere in considerazione i seguenti aspetti:

- spingere le persone a desiderare un cambiamento;
- porre in evidenza la possibilità di generare un cambiamento;
- individuare le azioni che consentono di produrre il cambiamento.

Le migliori strategie di intervento, nell' I.C. Marcheno sono di carattere prevalentemente preventivo:

- prevenzione universale: un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. EFFICACIA: gli effetti possono essere modesti se confrontati con programmi che trattano un gruppo con un problema specifico.
- prevenzione selettiva: un programma dedicato a un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini e segnalazioni fatte dalla scuola. EFFICACIA: gli effetti sono validi se la prevenzione universale non ha dato gli esiti previsti.
- prevenzione indicata: un programma di intervento sul caso specifico per dare supporto alle vittime o ridurre i comportamenti problematici. EFFICACIA: gli effetti sono positivi quando ci si avvale di professionalità diverse (es. psicologo dello sportello d'ascolto) e si coinvolgono anche le famiglie dei ragazzi.

La responsabilità dell'azione preventiva ed educativa chiama in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma non solo (istituzioni, associazioni, società sportive, etc.), ciascuna con un proprio compito nei confronti di bambini/e e di ragazzi/e. Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di questa collaborazione nasce, più o meno consapevolmente, dal riconoscimento sia da parte dei genitori che da parte degli insegnanti della rispettiva difficoltà a svolgere da soli la propria funzione formativa ed educativa.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di [cyberbullismo](#) e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
 - Ha il compito di coordinare le iniziative di prevenzione e contrasto del [cyberbullismo](#). A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
 - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il cyberbullismo è una variante del bullismo tradizionale. Secondo Chisholm "il cyberbullismo coinvolge bambini e adolescenti sia come vittime che come perpetratori in attività violente, pericolose e minacciose nel cyberspazio. Il cyberbullismo, a differenza del bullismo in cui il bullo si confronta faccia a faccia con la vittima, rinforza il danno alla cybervittima a causa della natura virtuale del cyberspazio; in esso, il bullo

può nascondersi dietro uno schermo, umiliare la vittima e divulgare materiale offensivo ad un vasto pubblico e in modo anonimo, senza la paura di essere scoperto e punito”.

Il cyberbullismo è:

- volontario: il comportamento è deliberato, non accidentale;
- ripetuto: non è incidentalmente isolato;
- dannoso: la vittima percepisce che il danno è stato inflitto;

Le caratteristiche peculiari del bullismo elettronico, rispetto a quello tradizionale, sono le seguenti:

- la convinzione dell'anonimato;
- l'impatto (la diffusione incontrollabile nella Rete);
- l'assenza di confini spaziali (non esistono più spazi-rifugio);
- l'assenza di confini temporali (contatto 24 ore su 24);
- l'assenza di supervisione da parte degli adulti;
- l'indebolimento dell'empatia (mancanza delle attivazioni dei "neuroni specchio");
- il feedback non tangibile (aumento del distacco tra gesto e significato perché il cyberbullo non vede le reazioni della vittima).

Il cyberbullismo è un fenomeno complesso che si manifesta con modalità articolate e si può distinguere in:

- **flaming**: invio di messaggi violenti e volgari allo scopo di suscitare conflitti verbali fra due o più utenti della rete;
- **harassment**: molestie attuate attraverso l'invio ripetuto di messaggi offensivi indirizzati verso la singola persona, che causano disagio emotivo psichico;
- **cyberstalking**: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità e non si sente più al sicuro neanche tra le mura domestiche;
- **denigration**: divulgazione all'interno di comunità virtuali - quali newsgroup, blog, forum di discussione, messaggistica immediata, siti Internet - di pettegolezzi e commenti crudeli, calunniosi e denigratori, allo scopo di danneggiare la reputazione o l'amicizia di colui che viene preso di mira;
- **tricy o outing estorto**: registrazione delle confidenze, raccolte all'interno di un ambiente privato creando un clima di fiducia, poi inserite integralmente in un blog

pubblico o in un social;

- **impersonation**: appropriazione dell'identità virtuale della vittima per compiere una serie di azioni che la porranno in difficoltà relazionali e in imbarazzo. Il furto di identità può avvenire a due livelli di complessità informatica: l'aggressore può aprire un nuovo profilo sui social network fingendo di essere la vittima oppure può agire come un vero hacker riuscendo ad insinuarsi nell'account della vittima;

- **exclusion**: estromissione intenzionale di un altro utente dal gruppo di amici, dalla chat o da un gioco interattivo;

- **sexting**: invio di messaggi via smartphone e Internet, corredati da immagini a sfondo sessuale;

- **happy slapping (schiaffo allegro)**: diffusione di un video dove la vittima è ripresa mentre subisce violenza psichica e fisica.

L'I.C. di Marcheno ritiene fondamentale che tutta la comunità scolastica costituita da docenti, personale ATA, alunni, genitori presti attenzione ai seguenti aspetti per riconoscere una potenziale vittima di cyberbullismo:

- appare nervosa quando riceve un messaggio o una notifica;
- sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);
- cambia comportamento o atteggiamento in modo repentino;
- mostra ritrosia nel dare informazioni su ciò che fa online;
- dopo essere stata online, mostra rabbia o si sente depressa;
- inizia a utilizzare sempre meno PC e telefono (arrivando a evitarli);
- perde interesse per le attività familiari e per le attività extrascolastiche che prima svolgeva;
- il suo rendimento scolastico peggiora.

Azioni del nostro Istituto

L'I.C. di Marcheno mira oltremodo a sensibilizzare gli utenti e a prevenire il fenomeno del cyberbullismo su tre livelli distinti:

- Azioni a livello individuale

- CONOSCENZA DEL FENOMENO

La conoscenza del cyberbullismo avviene attraverso la riflessione a partire dalle

seguenti domande-spunto:

- Quanto sono dipendente dallo smartphone? Che uso ne faccio? Per quante ore lo uso nell'arco della giornata? Riesco a darmi delle regole?
- Come la rete ha modificato il mio modo di comunicare e di pormi in relazione con l'altro? I gruppi whatsapp, la messaggistica sostituiscono il linguaggio verbale e non verbale?
- Quanto sono consapevole dei pericoli della rete, cosa penso di sapere, come penso di evitarli?

- MIGLIORAMENTO DELLE COMPETENZE DIGITALI DEL SINGOLO ALUNNO

Ciò avviene attraverso la riflessione a partire dalle seguenti domande-spunto:

- Conosco l'importanza di tutelare la mia privacy e quella degli altri (dati sensibili, password, foto, video) e cosa succede se trasgredisco?
- Conosco le regole o le norme etiche da tenere in mente quando si naviga in rete, quando si pubblica e/o si condivide un contenuto?

- POTENZIAMENTO DELL'AUTOSTIMA DI OGNUNO

- Azioni a livello di classe

- CONOSCENZA DEL FENOMENO DEL CYBERBULLISMO
- PROMOZIONE DI CONOSCENZA RECIPROCA, COESIONE, RISPETTO E RISOLUZIONE DEI CONFLITTO PER RAFFORZARE LA COESIONE INTERNA E IL RISPETTO DELLA DIVERSITA' (circle time, apprendimento cooperativo...)

- Azioni a livello d'istituto

- NOMINA DEL REFERENTE BULLISMO E CYBERBULLISMO, CHE COORDINA LE VARIE AZIONI
- SPORTELLO REFERENTE BULLISMO E CYBERBULLISMO (per l'a.s. 2020-21 a cadenza mensile)
- PROGETTO D'ISTITUTO SU ALCUNE CLASSI (quinta scuola primaria; prima, seconda, terza scuola secondaria)
- CONOSCENZA DEL FENOMENO (serate a tema, iniziative rivolte alle famiglie)
- GIORNATA NAZIONALE CONTRO IL BULLISMO E IL CYBERBULLISMO (7 Febbraio)
- SPORTELLO D'ASCOLTO CON PSICOLOGO
- DIFFUSIONE DI BUONE PRATICHE (vedi sito web della scuola)
- PATTO DI CORRESPONSABILITA' (vedi sito web della scuola)
- REGOLAMENTO D'ISTITUTO (vedi sito web della scuola)

L'I.C. di Marcheno prevede anche, sempre su tre livelli, le seguenti azioni di contrasto al fenomeno del cyberbullismo:

- Azioni a livello individuale

- RILEVAZIONE DEL FENOMENO ATTRAVERSO QUESTIONARI O TEST PER CONOSCERE COME L'ALUNNO SI TROVA IN CLASSE E A SCUOLA (<https://rb.gy/yurqof>)

- Azioni a livello di classe

- RILEVAZIONE DEL FENOMENO (ATTRAVERSO IL QUESTIONARIO E LE ATTIVITA' PROPOSTE DAL GRUPPO BULLISMO E CYBERBULLISMO: nomina dei pari, piramide della classe, termometro della classe, questionario "Come stai nella tua classe?")
- DISCUSSIONE E CONDIVISIONE DEI DATI RACCOLTI NEI CONSIGLI DI CLASSE E INTERCLASSE PER INDIVIDUARE STRATEGIE EDUCATIVE EFFICACI.

- Azioni a livello d'istituto

- REGOLAMENTO D'ISTITUTO
- VIGILANZA NEI LUOGHI E NEI MOMENTI PIU' A RISCHIO DI UTILIZZO DELLO SMARTPHONE PERSONALE (bagni, spogliatoi, intervallo, cambio dell'ora, entrata e uscita...).

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al

genere, all'orientamento sessuale, alla disabilità;

- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

COME RICONOSCERLO

L'odio si manifesta con un ampio spettro di azioni: sebbene tutte le espressioni che istigano all'odio meritino in una certa misura di essere classificate come malvagie, ne esistono tuttavia alcune che possono essere peggiori di altre; possono, ad esempio, essere più offensive, raggiungere e insultare un numero maggiore di persone, suscitare reazioni e passioni più forti, essere potenzialmente più dannose, ecc. Qualsiasi tentativo di contrastare il discorso dell'odio deve prendere in considerazione questi aspetti, poiché queste differenze di gravità determinano la risposta che si deve fornire. Per essere appropriate, le strategie di contrasto ai discorsi dell'odio non devono imporre restrizioni eccessive alla libertà di espressione, ma devono riconoscere i danni provocati (o che possono essere provocati) e cercare di porvi rimedio. Il seguente elenco propone alcuni aspetti utili da prendere in considerazione quando si valutano singoli episodi.

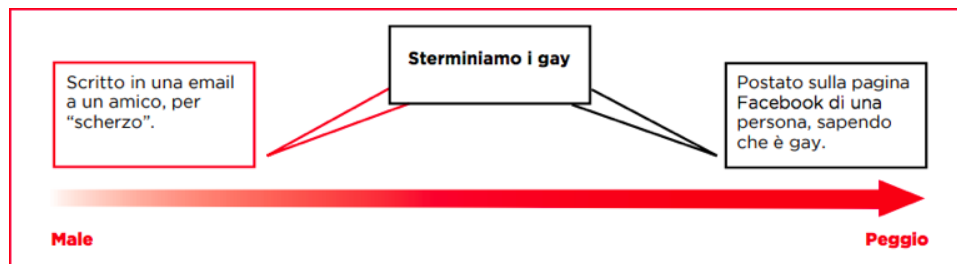
Il contenuto e il tono

Certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire. All'altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva (e perfino sotto falsa) luce.

Nella pratica, è molto difficile isolare il contenuto o il tono dal contesto generale. Se si prendono in considerazione altri fattori (qui di seguito) si può modificare il modo in cui sono classificate queste affermazioni.

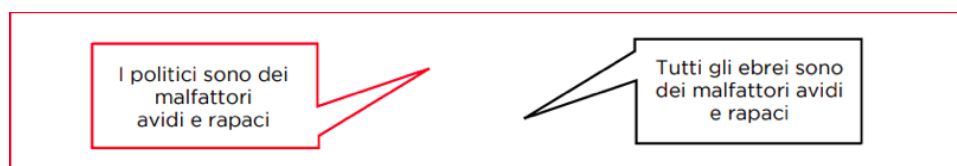
L'intenzione degli autori degli insulti

Ci può capitare di offendere gli altri senza volerlo, e poi di pentircene, e perfino di ritirare quanto abbiamo detto. Nei due esempi seguenti, entrambe le affermazioni sono intolleranti e sgradevoli, ma una è stata scritta con l'intenzione di offendere e fare del male.



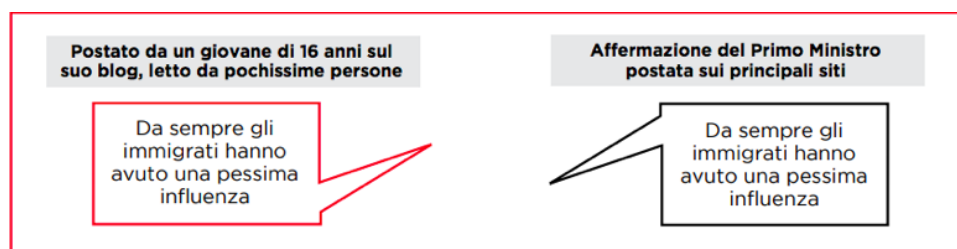
I bersagli o i bersagli potenziali

Alcuni gruppi, o individui, possono essere più vulnerabili di altri alle critiche. Può dipendere dal modo in cui sono globalmente considerati nella società, o da come sono rappresentati nei media, oppure dalla loro situazione personale, che non permette loro di difendersi efficacemente. L'esempio qui sotto mostra come la stessa espressione, applicata a gruppi diversi, possa avere un impatto molto diverso. Quella di destra rischia di essere molto più pregiudizievole.



Il contesto

Il contesto di una particolare espressione di odio è legato talvolta a circostanze storiche e culturali specifiche. Può includere altri fattori, come il mezzo utilizzato e il gruppo preso di mira, le tensioni o i pregiudizi esistenti, l'autorità del suo autore, etc.



L'impatto o l'impatto potenziale

L'impatto reale o potenziale esercitato sugli individui, sui gruppi o sull'insieme della società è una delle principali considerazioni da tenere presenti. Spesso, le ripercussioni negative subite dall'individuo o dal gruppo si rivelano più importanti della valutazione dell'episodio da parte di osservatori esterni.

COME INTERVENIRE

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono un ruolo centrale per la promozione della consapevolezza di queste dinamiche in rete.

Azioni del nostro Istituto

Azioni di educazione e sensibilizzazione:

- Adesione al [Manifesto della comunicazione non ostile](#) e darne visibilità sul sito dell'Istituto

Azioni di visibilità sul territorio:

- Organizzazione a livello di Istituto della Giornata contro il bullismo
- Organizzazione a livello di Istituto della Giornata contro il razzismo

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

La S.I.I.Pa.C., la Società Italiana Intervento Patologie Compulsive, definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete; di seguito alcune caratteristiche specifiche:

- **Dominanza.** L'attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.
- **Alterazioni del tono dell'umore.** L'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza.
- **Conflitto.** Conflitti inter-personali tra il soggetto e coloro che gli sono vicini,

conflitti intra-personali interni a se stesso, a causa del comportamento dipendente.

- **Ricaduta.** Tendenza a ricominciare l'attività dopo averla interrotta.

I segnali patologici di questo che viene descritto come **“un vero e proprio abuso della tecnologia”**, anche denominato **“Internet Addiction Disorder”** (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996), sono specifici così come accade per le altre dipendenze più “tradizionali”. In particolare, si hanno: la tolleranza, ossia quando vi è un crescente bisogno di aumentare il tempo su internet e l'astinenza quando, cioè, vi è l'interruzione o la riduzione dell'uso della Rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando s'interrompe o si riduce il comportamento). Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

Da sottolineare, la nomofobia (nomo deriva da “no-mobile”) termine usato per categorizzare quei soggetti che sperimentano emozioni negative, quali ansia, tristezza e rabbia quando non sono connessi con il proprio smartphone.

Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza dal gioco online (Net gaming addiction o Internet Gaming Addiction) inserito all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM 5). Da specificare che la dipendenza qui si realizza quando c'è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

Di seguito i sintomi che devono essere presenti (per un arco di tempo di almeno un anno):

1. il giocatore è assorbito totalmente dal gioco;
2. il giocatore è preoccupato e ossessionato dal gioco;
3. il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;
4. il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;
5. il giocatore sente di dover dedicare più tempo ai giochi;
6. il giocatore se non può giocare manifesta ansia, depressione e irritabilità;
7. può emergere un ritiro sociale;
8. il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;
9. il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;
10. il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet o ha perso interesse verso attività nella vita reale.

Anche in questo caso la scuola può indicare strategie per un uso più consapevole delle tecnologie per favorire il “benessere digitale”, cioè la capacità di creare e mantenere una relazione sana con la tecnologia.

La tecnologia infatti ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche online;
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali;
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

La scuola, attraverso azioni mirate, costruisce un percorso volto al benessere digitale degli studenti.

Azioni del nostro Istituto

- Riflessione personale degli studenti attraverso la compilazione di un questionario (sul tema del tempo on line e dei videogiochi) e successivo dibattito e riflessione collettiva in aula.
- Lettura e condivisione del regolamento sull'uso dei BYOD.
- Integrazione della tecnologia (anche ludica) nella didattica.

4.5 - Sexting

Il “sexting” è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti medialmente sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Il sexting (abbreviazione di sex - sesso e texting - messaggiare, inviare messaggi) indica l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri.

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di “revenge porn” letteralmente “vendetta porno” fenomeno

quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte. Tra le caratteristiche del fenomeno vi sono principalmente:

- **la fiducia tradita:** chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
- **la pervasività con cui si diffondono i contenuti:** in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;
- **la persistenza del fenomeno:** il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

Azioni del nostro Istituto

- Educazione all'affettività e alla sessualità.

4.6 - Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di **teen dating** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies - l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Potenziali vittime dell'adescamento online possono essere sia bambini che bambine, sia ragazzi che ragazze. Il fenomeno, infatti, non conosce distinzione di genere. Gli adolescenti sono particolarmente vulnerabili, poiché si trovano in una fase della loro vita in cui è molto importante il processo di costruzione dell'identità sessuale. Anche per questo potrebbero essere aperti e curiosi verso nuove esperienze e, talvolta, attratti da relazioni intime e apparentemente rassicuranti. In questa fase è importante, infatti, il bisogno di avere attenzioni esclusive da un'altra persona, di ottenere rinforzi esterni di approvazione per il proprio corpo e la propria immagine. È proprio in ragione della fiducia costruita nella relazione che le vittime di adescamento online riferiscono di sentirsi umiliate, usate, tradite e tendono a sentirsi in colpa e ad autosvalutarsi per essere cadute nella trappola.

Il processo di adescamento segue generalmente 5 fasi:

1. **Fase dell'amicizia iniziale:** Questa è la fase in cui l'adescatore cerca i primi contatti con la vittima individuata, provando a socializzare con lei. Tenterà, quindi, di conoscerla meglio al fine di scoprirne bisogni, interessi e il contesto in cui vive. Condividendo argomenti di interesse del minore l'adescatore cercherà pian piano di conquistarsi la sua fiducia, ponendogli domande frequenti che attestano interesse e attenzione nei suoi confronti. Gradualmente affronterà con la vittima argomenti sempre più privati ed intimi.
2. **La fase di risk-assessment:** in seguito ai primi contatti con il minore, l'adescatore cerca di comprendere il contesto in cui si svolge l'interazione (es. da dove si collega alla Rete? I genitori lo controllano quando chatta? Che rapporto ha con loro?). L'obiettivo dell'adescatore è quello di rendere sempre più privato ed "esclusivo" il rapporto, cercando di passare, ad esempio, da una chat pubblica ad una privata, da una chat alle conversazioni attraverso il telefono, per poterne così carpire il numero.
3. **Fase della costruzione del rapporto di fiducia:** le confidenze e le tematiche affrontate divengono via via più private ed intime o comunque molto personali. In questa fase l'adescatore può iniziare a fare regali di vario tipo alla vittima e

può anche avvenire lo scambio di foto, subito e non necessariamente a sfondo sessuale.

4. **Fase dell'esclusività:** l'adescatore rende la relazione con il minore sempre più "segreta", isolandolo sempre più dalla famiglia e dagli amici. Chiederà alla vittima di non raccontare a nessuno ciò che sta vivendo. L'esperienza reciproca verrà presentata come un "geloso segreto" da custodire per non rovinare tutto. In questa fase l'adescatore potrà ricorrere a ricatti morali puntando sulla fiducia costruita, sulla paura o sul senso di colpa.
5. **Fase della relazione sessualizzata:** in questa fase la richiesta di immagini o video sempre più privati e a sfondo erotico potrebbe essere più insistente, così come la proposta di incontri offline. Qualora il minore avesse già inviato immagini o video privati, potrebbe essere ricattato dall'adescatore: se non accettasse un eventuale incontro l'adescatore potrebbe diffondere quel materiale online. Questi, inoltre, tenderà a presentare sempre la situazione come "normale" al fine di vincere le eventuali resistenze del minore a coinvolgersi in tale rapporto.

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore.

Ecco alcuni segnali e domande che potrebbero esserci di aiuto nell'identificazione del fenomeno:

- Il minore ha conoscenze sessuali non adeguate alla sua età?
- Venite a conoscenza di un certo video o di una foto che circola online o che il minore ha ricevuto o filmato, ma c'è imbarazzo e preoccupazione nel raccontarvi di più...
- Il minore si isola totalmente e sembra preso solo da una relazione online?
- Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

Azioni del nostro Istituto

- Collaborazione con gli enti del territorio;
- Interventi in classe delle Forze dell'Ordine o esperti del settore.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente

espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *“Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù”*, introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella **legge n. 38 del 6 febbraio 2006** *“Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet”*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest’ultima, introduce, tra le altre cose, il reato di “pornografia minorile virtuale” (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

In un’ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d’età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un’attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **“Segnala contenuti illegali” (Hotline)**.

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il “Clicca e Segnala” di [Telefono Azzurro](tel:112) e “STOP-IT” di [Save the Children](http://www.savethechildren.it).

Se si ravvisa un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e coinvolte nella visione di contenuti pedopornografici sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o

pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato - Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato - Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri - Comando Provinciale o Stazione del territorio di competenza.

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità.

L'abuso sessuale online rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale online si manifesta producono effetti sulle vittime che si aggiungono e moltiplicano a quelli associati all'abuso sessuale.

Azioni del nostro Istituto

- Sensibilizzazione verso i problemi derivanti della diffusione in rete della immagine propria e altrui
- educazione all'affettività e sessualità
- attivazione di spazi di ascolto a cura dei Servizi del territorio

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

- ☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- ☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso.**
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

- **Cyberbullismo:** è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per

segnalare la presenza di materiale pedopornografico online.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) - Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) - Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;

- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:1.96.96).

Nel caso A l'insegnante prevalente o il coordinatore di classe dovrebbe consultare il referente d'Istituto per il contrasto del cyberbullismo per valutare le possibili strategie d'intervento, anche avvalendosi del manuale delle attività elaborato dal gruppo bullismo dell'I.C., consultabile nel sito istituzionale. Se si ravvisa l'urgenza, è possibile anche coinvolgere il Dirigente Scolastico.

Nel caso B il l'insegnante prevalente o il coordinatore di classe deve informare immediatamente il Dirigente Scolastico e il referente d'Istituto per il contrasto del cyberbullismo che valuteranno insieme le possibili strategie d'intervento. Se non si ravvisano fattispecie di reato, si dovrebbe:

- informare i genitori degli studenti direttamente coinvolti;
- richiedere, in concomitanza, ove si ritiene opportuno, la consulenza dello psicologo dello Sportello d'Ascolto;
- informare i genitori degli alunni che non hanno compiuto 14 anni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori dei siti internet o social (o successivamente, in caso di non risposta entro 48 ore, al Garante della Privacy);
- convocare il consiglio di classe;
- richiedere, se opportuno, il sostegno di associazioni o enti esterni se l'azione di cyberbullismo ha avuto impatto sulla vita quotidiana della vittima.

A seconda delle valutazioni fatte dal team/consiglio di classe insieme al Dirigente scolastico, al referente e ai genitori, si potrebbe poi segnalare il caso alla Polizia Postale.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse “Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani” (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

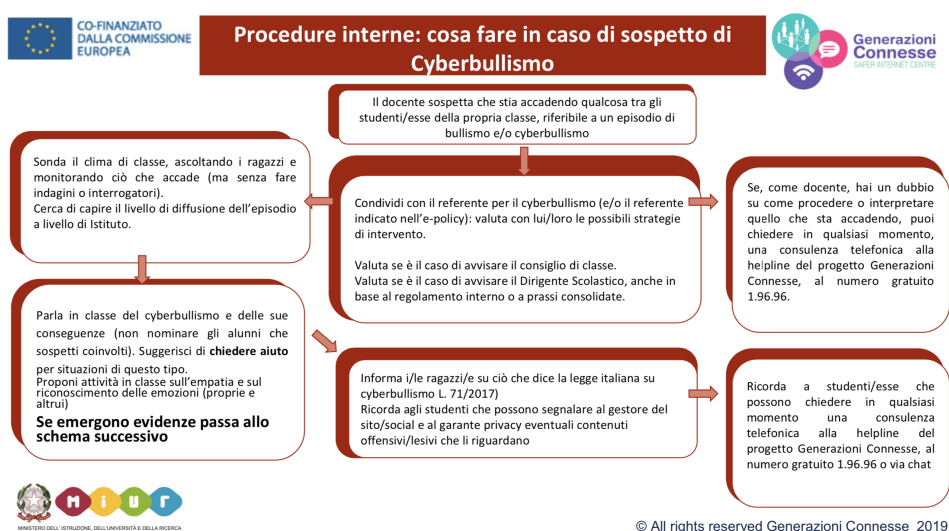
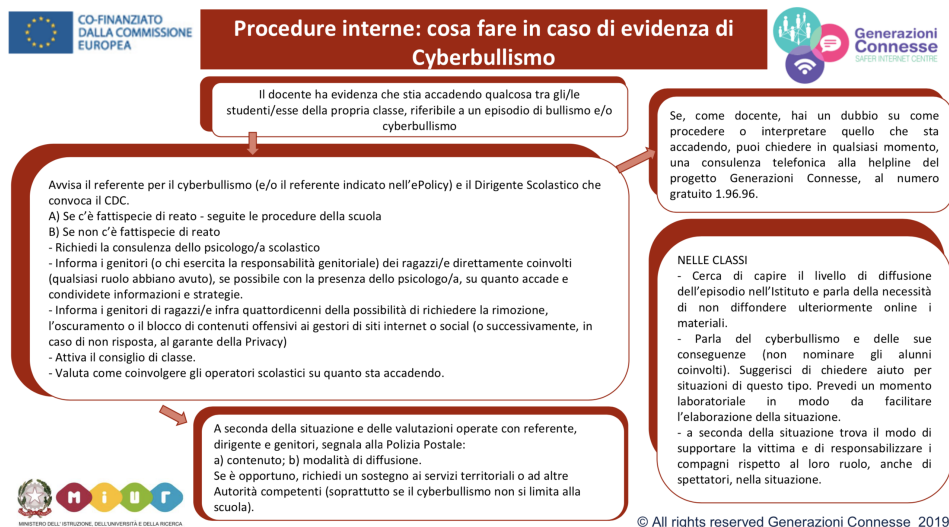
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

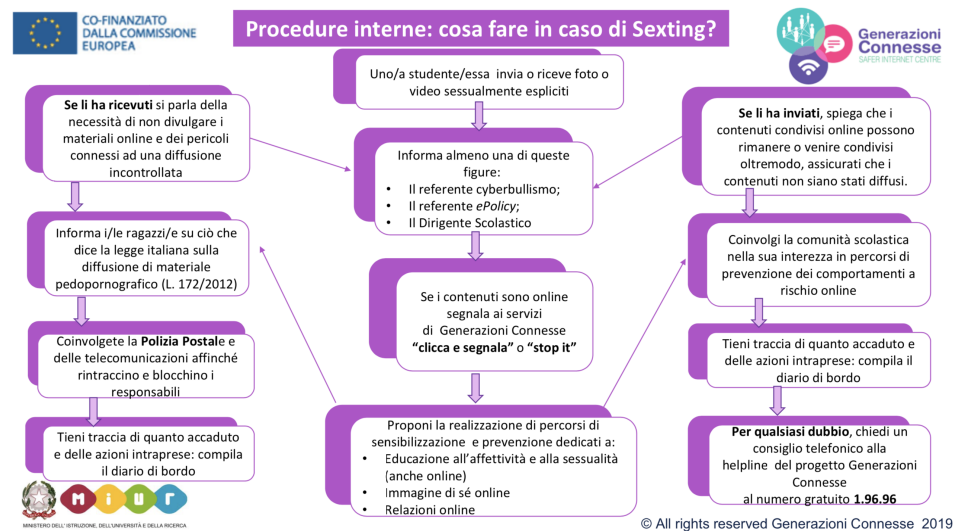
A livello locale l'Istituto si avvarrà della collaborazione dell'associazione Civitas operante sul territorio.

5.4. - Allegati con le procedure

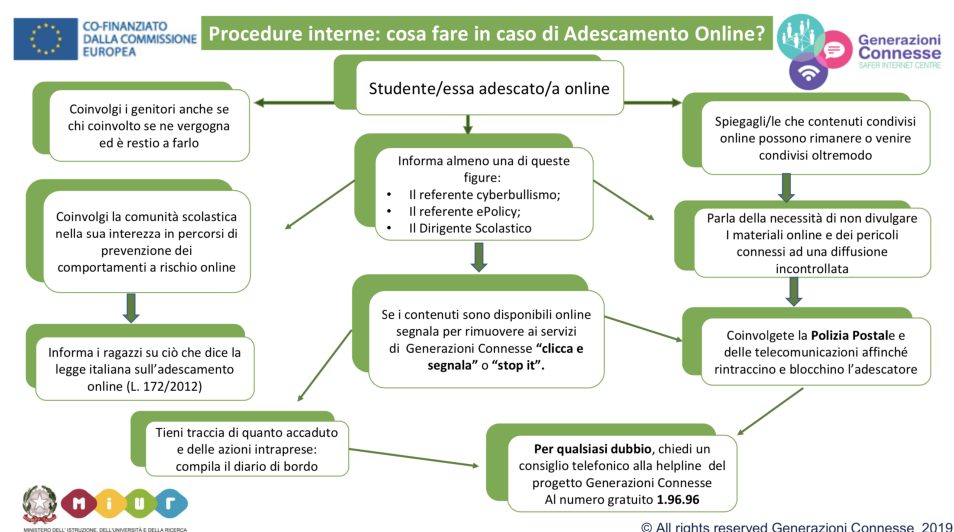
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



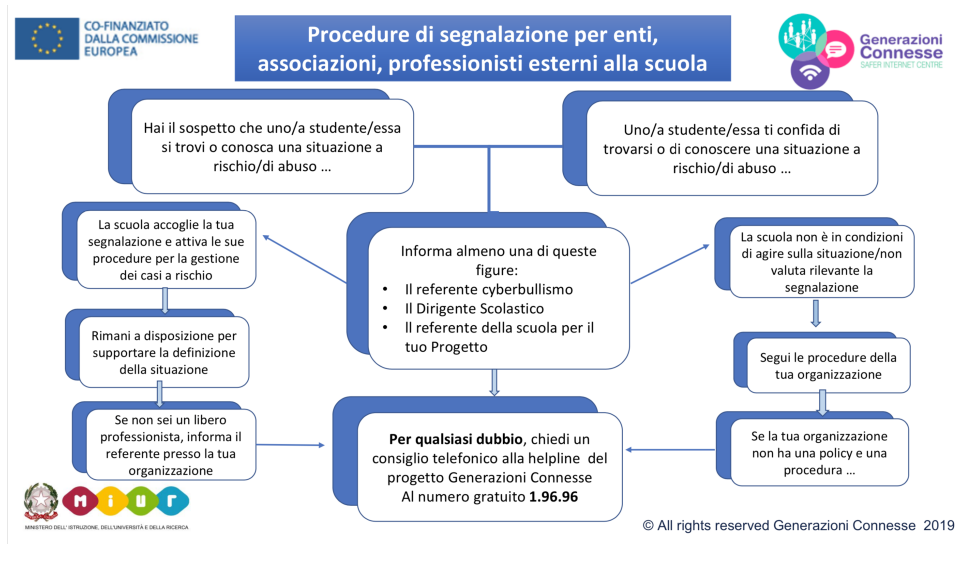
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Altri allegati

- [Scheda di segnalazione](#)
- [Diario di bordo](#)
- [iGloss@ 1.0 l'ABC dei comportamenti devianti online](#)
- [Elenco reati procedibili d'ufficio](#)

Per rendere più agevole la procedura agli insegnanti che si trovassero all'interno delle situazioni descritte, l'Istituto di Marcheno propone le seguenti tabelle riassuntive:

IL DOCENTE SOSPETTA UN CASO DI CYBERBULLISMO

CON CHI PARLARE?

- COLLEGHI DI CLASSE
- REFERENTE CYBERBULLISMO PER MATERIALI UTILI O CASISTICA
- DIRIGENTE SCOLASTICO
- IL DIRIGENTE DECIDE SE INFORMARE I GENITORI

COSA FARE IN CLASSE?

- NON NOMINARE IL SOGGETTO CON LA CLASSE
- SUGGERIRE ALLA CLASSE COMPORTAMENTI POSITIVI E NEGATIVI CITANDO CASI PARADIGMA
- LAVORARE SULL'EMPATIA E SUL GRUPPO
- RICORDARE AGLI STUDENTI LA LEGGE AL RIGUARDO

IL DOCENTE HA RILEVATO UN EVIDENTE CASO DI CYBERBULLISMO

CON CHI PARLARE?

COSA FARE IN CLASSE?

- DIRIGENTE SCOLASTICO E REFERENTE CYBERBULLISMO
- IL DIRIGENTE CONVOCA CONSIGLIO DI CLASSE
- AVVISARE CON IL DIRIGENTE LE FAMIGLIE
- APPOGGIARSI AD ASSOCIAZIONI DI SUPPORTO
- AVVISARE POLIZIA POSTALE SE C'E' FATTISPECIE DI REATO
- SONDARE IL CLIMA DEL GRUPPO X COMPRENDERE LA DIFFUSIONE DEL FENOMENO
- PUNTARE SULL'IMPORTANZA DI NON DIFFONDERE ULTERIORMENTE MATERIALE, NOTIZIE...
- SENZA DIFFONDERE DATI SENSIBILI, SOSTENERE LE VITTIME E INDIRIZZARLE VERSO ASSOCIAZIONI DI SUPPORTO

IL DOCENTE HA RILEVATO UN CASO DI SEXTING O ADESCAMENTO ON-LINE (UN ALUNNO RICEVE O INVIA MATERIALI SESSUALMENTE ESPLICITI, UN ALUNNO VIENE ADESCATO IN RETE E IL DOCENTE NE VIENE INFORMATO)

COSA FA IL DOCENTE?

- INFORMA IL DIRIGENTE O IL REFERENTE EPOLICY
- HA CURA CHE IL MATERIALE NON SI DIFFONDA ULTERIORMENTE
- INFORMA I GENITORI
- INFORMA I RAGAZZI SULLE CONSEGUENZE LEGALI DI TALI AZIONI (L.172 - 2012)
- PROPONE ALLA CLASSE PERCORSI DI ED. ALL'AFFETTIVITA' E ALLA RIDEFINIZIONE DELL'IMMAGINE DI SE' E DELLE RELAZIONI ON-LINE
- TIENE UN DIARIO DI BORDO DELLA SITUAZIONE (vedi allegato)
- SEGUE PROCEDURA DI SEGNALEZIONE PER I CASI A RISCHIO
- INFORMA LA POLIZIA POSTALE PER RINTRACCIARE O BLOCCARE L'ADESCATORE

Il nostro piano d'azioni

Non è prevista nessuna azione.

